What is claimed is:

1. A method of regulating access to a website by a user terminal via the internet, the user terminal reading a document including an embedded digital watermark, said method comprising the steps of:

at the user terminal, extracting identifying data from the digital watermark, and providing the identifying data to a central computer;

at the central computer:

identifying a pointer associated with the identifying data;

generating a validation key; and

providing the pointer and the validation key to the user terminal;

at the user terminal, communicating with the website via the pointer and providing the validation key to the website; and

at the website, regulating access to the website by the user terminal based at least in part on the validation key.

2. The method according to claim 1, wherein the identifying data comprises a document identifier.

3. The method according to claim 2, wherein the pointer comprises at least one of a URL, IP address and web address.

4. The method according to claim 2, wherein the validation key comprises a date-time value.

5. The method according to claim 2, further comprising the step of encoding the validation key.

6. The method according to claim 5, wherein the encoding comprises at least one of hashing, encrypting, and rotating.

7. The method according to claim 5, wherein the encoding comprises converting a validation key to alpha-characters, and adjusting the characters according to a code key.

8. The method according to claim 7, further comprising the step of encoding the code key with the validation key.

9. The method according to claim 1, wherein the validation key comprises at least one of a predetermined number and a pseudo-random number.

10. A method of authenticating permission to access a system comprising the steps of:

receiving a request to enter the system, the request including at least a validation key;

determining whether the validation key is valid; and

allowing access to the system based on a determination of said determining step.

11. The method according to claim 10, wherein said system comprises a website.

12. The method according to claim 10, further comprising the step of decoding the validation key.

13. The method according to claim 10, wherein the validation key comprises a timestamp, and said determining step determines whether the timestamp is stale.

14. The method according to claim 10, wherein the validation key comprises a timestamp, and said determining step determines whether the timestamp is within a predetermined range.

15. The method according to claim 10, wherein the validation key comprises a predetermined number, and said determining step determines whether the predetermined number matches at least one number on a list of numbers.

16. The method according to claim 10, wherein the system provides information related to a digitally watermarked document.

17. The method according to claim 10, further comprising a step of determining whether the validation key comprises a valid value.

18. The method according to claim 17, wherein said validation key comprises a timestamp, and step of determining whether the validation key comprises a valid value includes determining whether the timestamp has a predetermined format.

19. The method according to claim 10, wherein the request includes a URL and the validation key is appended to the URL.

20. A method of authenticating permission to access a website via the internet, said method comprising the steps of:

receiving a request to enter the system, the request including at least a validation key,

determining whether the validation key has been previously received; and

allowing access to the system based on a determination of said determining step.

21. The method according to claim 20, wherein the validation key includes at least one of a date-time value, a pseudo-random number and a predetermined number.

22. The method according to claim 21, wherein said determining step comprises the steps of querying a database to determine if the validation key is stored therein.

23. A method according to claim 21, further wherein the request comprises a URL identified from a digitally watermark-based system.

24. A system for exchanging data comprising:

a central server comprising at least one database including pointer information, wherein when a user terminal communicates an extracted watermark identifier to said central server, said central server identifies a corresponding pointer associated with the extracted watermark identifier, and wherein said central server generates a validation key and encodes the validation key, and wherein said central server appends the validation key to the corresponding pointer, and communicates the pointer and validation key to the user terminal.

25. The system according to claim 24, wherein the pointer comprises at least one of a URL, IP address and web address.

26. The system according to claim 25, wherein the validation key comprises a date-time value.

27. The system according to claim 24, wherein said central server encodes by at least one of hashing, encrypting, and rotating.

28. The system according to claim 27, wherein the central server encodes by converting the validation key to alpha-characters, and adjusting the characters according to a code key.

29. The system according to claim 28, wherein the central server encodes the code key with the validation key.

30. The system according to claim 24, wherein the validation key comprises at least one of a predetermined number and a pseudo-random number.

31. A method of operating a computer server, the computer server to communicate with at least one user terminal, said method comprising the steps of:

receiving a document identifier from the user terminal;

identifying a pointer associated with the document identifier;

determining whether the pointer is a predetermined class, and

if not the predetermined class, communicating the pointer to the user terminal; and

if the predetermined class, generating a validation key, and communicating the pointer and validation key to the user terminal.

32. The method according to claim 31, wherein the pointer comprises at least one of a URL, IP address and web address.

33. The method according to claim 32, wherein the predetermined class comprises at least one of a restricted access website, exclusive access website, an entry-through-purchased documents website, a restricted URL, and an exclusive URL.

34. The method according to claim 33, wherein the validation key comprises at least one of a time stamp, a predetermined number, and a pseudo-random number.

35. The method according to claim 34, wherein said document identifier comprises an identifier extracted from a digitally watermarked document.

36. The method according to claim 35, further comprising the step of encoding the validation key.

37. The method according to claim 34, wherein said document identifier comprises an identifier extracted from a digitally watermarked document.

38. A computer server, said computer server to communicate with at least one user terminal, said computer server comprising:

means for receiving a document identifier from the user terminal;

means for identifying a pointer associated with the document identifier;

means for determining whether the pointer is a predetermined class, and

if not the predetermined class, means for communicating the pointer to the user terminal; and

if the predetermined class, means for generating a validation key, and communicating the pointer and validation key to the user terminal.